RADIO TV REPORTS, INC.

4701 WILLARD AVENUE, CHEVY CHASE, MARYLAND 20815 656-4068

FOR PUBLIC AFFAIRS STAFF

PROGRAM American Interests STATION WETA-TV PBS Network

DATE May 5, 1983 10:30 P.M. CITY Washington, D.C.

SUBJECT Technology Piracy

WILLIAM SCHNEIDER: Today there continues to be a serious threat to our national security from Soviet technology piracy, in which an increasing one-way stream of U.S. technology is moving to the Soviet Union.

PETER KROGH: The Soviets are modernizing their military through a vast flow of high-technology from the West. The Administration calls it a hemorrhage that must be stopped. But critics say the government is overreacting with policies that will cripple U.S. industry's hottest exports and blunt America's edge on the newest frontier of world trade.

REP. DON BONKER: For some people, it's a hemorrhage. To others, it's harassment of the business community.

KROGH: The Soviet military bloc has an edge over the West in sheer numbers, fielding more troops, more tanks, more planes, more missiles. The Western Alliance confronts this challenge with superior technology. Its arsenal is more advanced, its weapons presumed more effective, many of them combat-proven on the battlefields of the Middle East. It is through this primacy in technology that the West maintains the balance of military power.

RICHARD PERLE: In the last several years we have suffered a serious loss of technology from the West. This has shown up in the form of the increasing sophistication of Soviet military equipment.

KROGH: Alarms about growing Soviet military might are a standard feature of Washington's politics. How serious is this threat? Very serious, according to the Democrats on the Senate

Investigations Committee. They found that priceless U.S. technology has made its way to Moscow, contributing to giant strides in Soviet military strength. Ominous, accoding to the intelligence community, whose first detailed study of the loss of strategic technology revealed, quote, Western technical superiority is eroding, as the Soviet Union and its allies introduce more and more sophisticated weaponry, weapons that all too often are manufactured with the direct help of Western technology.

Among the examples cited were a new scheme for hardened missile silos, clearly patterned after American designs; the rapid development of the Ilyushin-76, a large military transport with obvious similarities to the American C-141; and catapult systems like those used on American carriers, common throughout the West, but, to quote the CIA, beyond Soviet naval experience.

In fact, much of the technology the West takes for granted is beyond Soviet capabilities. According to one official charged with frustrating Moscow's acquisition efforts:

WILLIAM VON RAAB: Right now the Soviet Union is incapable of fulfilling its own ambitious military production goals. They know they need Western technology, and know specifically what technology they need.

KROGH: In other words, Western technology is a necessity for the Soviets, not a luxury. The CIA's national intelligence officer for science and technology explains why.

JAN HERRING: Although the Soviets do have good scientists and engineers, their political-economic system is not conducive to technological innovation.

Take a look at the civil sector. Their oil and gas, their chemicals, their agriculture, and even their automotive industry requires large amounts of Western technology to be productive. In fact, the military sector in the Soviet Union even needs higher levels of technology to produce the high-performance weapons that their military planners demand.

KROGH: Technology requiring an investment of hundreds of millions of dollars and years of research, except that the Soviets have found a shortcut.

SCHNEIDER: The Soviet technological gains obtained through a carefully crafted acquisition program are providing them with significant savings in time and money in their military research and development programs, rapid modernization of their defense industrical infrastructure, the closing of gaps between our weapons systems and theirs.

KROGH: As a requirement for military modernization, Moscow's pursuit of Western technology is not left to chance. According to the CIA, the Soviet effort is massive, well-planned and well-managed, a national-level program approved at the highest party and governmental levels.

In this CIA diagram of the Soviet bureaucracy, all the ministries in blue are known to be heavily involved in procuring Western technology, six ministries in all, employing as many as 20,000 party cadre in such work. At least one entire ministry does nothing but pursue technology from the West.

DR. IGOR GLAGOLEV: The State Committee on Science and Technology [unintelligible] depends on studies, is devoted almost exclusively to the acquisition of Western technology and...

KROGH: Before he defected in 1976, Dr. Glagolev was an adviser to the Soviet Politburo and the Central Committee of the Communist Party, as well as a section director in the Academy of Sciences. Based on his experience, he told Congress to ban the transfer of all technology to the Soviets.

DR. GLAGOLEV: All kinds of technology which are required from the West are used first of all for the military purposes and for the purposes of the KGB, because these two situations have the first priority in the Soviet Union.

KROGH: It is the KGB, the Committee for State Security, which oversees the entire Soviet effort to acquire Western technology. It is a responsibility not likely to be diluted now that Yuri Andropov, former head of the KGB, presides in the Kremlin.

VON RAAB: Their success, until lately, has been alarming for us, but certainly most gratifying for them. They have acquired computers, lasers, guidance and navigation systems, structural materials, and microprocessors, just to name a few.

But all their acquisitions have two things in common. They have military value and they were acquired with relative ease.

KROGH: In fact, some of Moscow's most valuable acquisitions have been obtained openly and legally through trade by purchasing items ostensibly for civilian use and diverting them to the military. Three examples:

In 1972 the Soviets scored a major breakthrough in missile accuracy by purchasing American machinery to manufacture industrial ball bearings, the kind of high-speed precision ball bearings that are also critical to the development of ICBM guidance systems.

A few years later, Japan sold the Russians two huge floating drydocks, quite beyond the production capability of any Soviet shipyard. The Russians diverted them to the servicing of their newest aircraft carriers.

And then there was the Kama River truck plant, the world's largest and most sophisticated, built with American technology and credit. In 1979 the Soviet Army invaded Afghanistan on the wheels of American know-how.

It was Afghanistan which promoted the first U.S. efforts to ban the sale of all advanced technology to the Soviets. But the legal trade of technical hardware is only one source of technology for Moscow. Raw scientific data is another. As the CIA points out, an open society provides countless opportunities for information-gathering.

HERRING: From the hundreds of cases of military-significant technology that we have studied, we have found that something of the order of 70 percent had been acquired by Soviet intelligence operations, both overt and clandestine. On the other hand, we believe that the remaining 30 percent of the acquired military-
significant technology is just as important. It comes from open-source publications, from student exchanges, and from just the uncontrolled sale of technology on a worldwide basis.

KROGH: What they cannot buy, the Soviets can often learn about in other ways. Critical information is readily available at scientific trade fairs and professional gatherings, in popular magazines, technical journals, and government publications, and through the Freedom of Information Act.

SENATOR SAM NUNN: What I think is ridiculous is that our Freedom of Information Act is now so broad that if Qaddafi of Libya wrote in and demanded of the government that he be given access to certain unclassified information, he could get it. If Andropov, the head of the Soviet Union, wrote in and signed his own name and title, under our Freedom of Information Act, he is absolutely entitled to it.

KROGH: Finally, according to Dr. Miles Costick, an expert on Soviet industrial espionage, the Soviets tap universities and private research institutes.

DR. MILES COSTICK: For instance, Massachusetts Institute of Technology was one of the principal targets because it is known as a defense contractor and doing classified work for the United States defense community. The inertial navigation system for the United States intercontinental ballistic missiles and intercontinental bombers was developed in the mid- and late '60s at the MIT.

KROGH: The prime concern of the intelligence community, however, lies elsewhere.

HERRING: There has been some military-significant technologies acquired from our universities. But in the most part, it's been a very small part of this transfer flow.

KROGH: The real hemorrhage, fully 70 percent of what the Soviets acquire, is the result of espionage.

October 1982. The Swedish Navy searches in vain for what it thinks is a Soviet submarine prowling near a highly classified military base. The sub eludes them. The reason, according to one authority, is that it was a new mini-sub with some extraordinary characteristics.

DR. COSTICK: One of them was that it could dive deeper, all the way to the ocean floor, at depths which no military submarine could have ever reached.

Number two, those submarines, being small and not having magnetic properties, could not be detected by the traditional anti-submarine warfare technology.

KROGH: Such a submarine does exist. The technology was developed for civilian deep sea research by an American firm, then purchased by a Canadian company. By law, it could not be exported to the Soviet Union. But the Russians got hold of it anyway.

DR.COSTICK: How were they able to acquire this technology? Well, they have gone to the firm and made an offer which was difficult to refuse. They were prepared to pay several times the price. However, the export license which was required for such a submarine and such a technology was denied. The Soviets set up a dummy firm in Switzerland. And export of such an item to Switzerland would not be controlled because Switzerland is not a controlled country. That particular firm came and bought this submarine from the Canadian firm. It was dismantled, placed into crates, shipped via air freight to Zurich, Switzerland, where it was immediately re-routed to the Aeroflot -- namely, the Soviet government airlines -- and shipped to the Soviet Union.

KROGH: The U.S. to Canada to Switzerland to Russia. Such diversion schemes are all too typical, according to the Commerce Department's new Office of Export Enforcement, which is trying to stop them.

THEODORE WU: The Soviet Union and the East Bloc countries, individually and collectively, want to get their hands on U.S.-origin and other Western-origin technologies. And we can see

that especially in the last couple of years that the number of suspected illegal transactions, as well as clearly unlawful export of controlled technologies, are on the rise.

KROGH: As a former U.S. attorney in California, Theodore Wu had his own close encounter with such practices. In 1980 he helped convict the president of an optical company who sold laser mirrors like these to the Russians. They look harmless, but they're similar to those developed for the Air Force flying laser laboratory for experiments in anti-missile defense systems. In this case, the initiative was taken by an American businessman. But usually Soviet agents have to be more aggressive.

WU: They gave so-called shopping lists as to what items they want to get and when they want to get these items, how much they are willing to pay to get these items. And indeed, they have very good information as to who manufacture some of these items and where these manufacturers are located, and what security safeguard, if any, do these manufacturers have.

KROGH: The current Soviet shopping list includes advanced computers; microelectonics, including machinery for manufacturing high-speed integrated circuits; and, of course, laser technology for the development of Star Wars type anti-missile and anti-satellite systems.

This is the world of high technology. And in the United States, two regions in particular have become centers of high-tech industry, the East Coast between Boston and Washington, D.C., and the West Coast, especially a 30-mile strip just south of San Francisco known as Silicon Valley. Nearly 1500 companies are clustered here, including some of the largest in the high-tech field. This is the home of the silicon microchip, perhaps the epitome of what is called dual technology. Dual because microchips are not only the brains of civilian calculators and computer games, but of the most advanced weapons, as well.

Advanced military technology, reflecting its dual civilian and military use, is now developed by private companies, often operating in vulnerable industrial parks like these rather than in closely guarded government plants. Ask anyone who believes there is a technology hemorrhage where it starts, and the answer is the same.

SENATOR NUNN: I think the greatest area is probably in the private sector and in areas where the Department of Defense is not directly involved.

HERRING: These companies oftentimes are not capable of protecting themselves against the HUMINT penetration operations of the Soviet bloc.

KROGH: Until very recently, most private companies paid little heed to security measures. So as much as $20 million worth of microelectronic gear has been stolen each year just from California's Silicon Valley alone. Much of it ends up on the black market or in what local police call a gray market of semi-legal trade. But for the Russians it's often more like a supermarket.

For example, Werner Bruckhausen, thought to be an East German agent, funneled an estimated $9 million worth of electronics to the Soviet bloc by purchasing large quantities of such stolen goods. He smuggled them out through a network of phony corporations, part of an international web of some 400 dummy firms spun by the Soviet bloc throughout the West.

There are also more traditional espionage cases. Marian Zakarski was a Polish spy masquerading as vice president of a firm owned by the Polish government. He enticed and bribed William Bell, a disenchanted engineer at Hughes Aircraft, into divulging critical information on America's newest warplanes, like the F-15, the B-1 bomber, the Stealth bomber, and several types of missiles.

The Pentagon estimates that Moscow meets 50 percent of its needs for strategic technology through espionage conducted by 3000 special field agents. For the FBI, it's an increasing headache.

EDWARD O'MALLEY: Not only are the activities by the Soviets increasing, but the activities of their surrogates here in the United States -- and when I say surrogates, I mean the Eastern European intelligence services -- are on the increase also.

JOHN MCGUIRE: His story was that he was a Belgium businessman doing business in Russia, and they were pressuring him for a long time.

KROGH: John McGuire was the target of what started out as an indirect approach by the Soviets. McGuire is president of a Virginia-based firm called Software A.G. of North America, which produces computer programs for classified use. The key to unscrambling these programs is called a source code.

MCGUIRE: It's analogous to the chemical formulas or a Coca-Cola formula. You can drink the Coke, but you don't understand what the process was to produce that liquid.

KROGH: Among the customers for McGuire's system are the CIA and the Marine Corps. The Russians wanted McGuire's source code.

MCGUIRE: It would save them ten years in understanding the most advanced version of data base management. It would have collapsed the time necessary to achieve that sophistication on their own computers.

KROGH: McGuire was offered nearly half a million dollars for the code by a Belgian, Mark Degeiter, who admitted he'd sell it to Moscow. McGuire called the FBI.

MCGUIRE: Under guidance of the FBI, they got a court order, they tapped my phone, they put a video camera in my office. We were trying to get Degeiter to come in here and discuss the situation. He was flitting around the country and over in Russia and Europe, out in Silicon Valley in California. And so I had a lot of phone conversations with him over that period of time, maybe 30 or 40. At which point, we were negotiating. For example, he wanted me to deliver the source code in Belgium and get paid off in Switzerland in cash. And, of course, the FBI wanted the transaction to take place under surveillance in the United States, so that we could apprehend him.

KROGH: Because of McGuire's cooperation and perseverance, the FBI finally nabbed Degeiter. But at FBI Headquarters, the realization that such cooperation is far too rare and industrial security much too lax led to DECA, Development of Counterintelligence Awareness, a program to alert more than 11,000 private firms with defense contracts to the danger of espionage.

O'MALLEY: It's a program where, having identified these firms, we'll go out and we'll talk to them. We'll talk to them about our own responsibilities in the counterintelligence area and how they can be of assistance to us, and perhaps how we can be of assistance to them. And we'll also tell them about the threat posed by the intelligence services of the hostile countries and others.

KROGH: But the FBI's DECA program is only a small part of the government's plan to halt technology leaks, and the only part that isn't controversial.

VON RAAB: Through Operation Exodus, the United States has begun the first major systematic effort to keep critical technology out of the hands of potential enemies, while facilitating trade and commerce with trading partners abroad.

KROGH: There are some 300 ports, airfields and roads through which to smuggle technology out of the United States. Exodus is trying to cover all of them, including Baltimore Harbor. It's a new rule for Customs, which traditionally

monitors what comes into the country. Now nearly 300 special agents and inspectors are keeping tabs on what goes out.

But dockside inspections are only a part of the operation. Like the FBI's DECA program, each local office is responsible for checking out nearby companies, to educate them and gather information about them.

Senior inspector Steven Knox explains how it's done.

STEVEN KNOX: We go through the exprt register item-by-item. We will go through communications systems item-by-item.

Here's one which manufactures underwater communications systems. Our primary question would be, "What is the sophistication of the underwater communications system?" because it could be such things as for submarine use, obviously, for naval use. We will go out. We will pay them a visit.

KROGH: The Exodus program is the cutting edge of a campaign to control the illegal export of high technology. It is also a magnet for controversy. Congressman Don Bonker tried to close down the Exodus program in Seattle and Portland when exporters complained that legitimate shipments were being subjected to costly delays.

REP. BONKER: Opeation Exodus is a new and, I think, unwarranted dimension to the enforcement program under the Export Administration Act. There was no Operation Exodus a few years ago. It was conceived in the White House and funded by the Department of Defense. And now they're coming to Congress, asking for $30 million to carry out an enforcement function that is already being implemented by the Department of Commerce.

KROGH: But when it comes to deterring illegal exports, the Commerce Department has not done its job, according to critics, who charge that because the department's main function is to promote trade, it is ill-equipped and uninclined to police its own customers, the export industry.

Commerce has responded to this charge by creating a new Office of Export Enforcement, headed by Theodore Wu, who has been defending his efforts before Congress.

WU: And we are now well on the way to becoming a highly specialized, trained export enforcement investigative arm that is well supported by intelligence operations.

KROGH: But Wu has not pacified the critics, including Senator Sam Nunn, whose 18-month investigation of technology leaks led him to propose transferring all law enforcement

functions to Operation Exodus and its experienced personnel from the Customs Service.

SENATOR SAM NUNN: So this is right up the alley of Customs. It's what they've been doing for years and years. And I think it makes all sorts of sense to put law enforcement functions in an agency that has law enforcement history and background and capability.

KROGH: The trade industry has been aroused by the Exodus controversy, knowing that it masks a profound policy dispute over export controls now being fought out within the Administration.

FILM NARRATOR: CBEMA, the Computer and Business Equipment Manufacturers Association, is the voice of our industry in Washington, D.C.

KROGH: Trade organizations such as CBEMA are fighting rigid export controls that they fear will squeeze them out of the world market without impairing Moscow's access to advanced Western technology.

FILM NARRATOR: Remove export barriers for all products and services that are not subject to genuine national security interests.

KROGH: They are especially upset by the Administration's failure to revise the Pentagon's list of critical military technology, items barred from export because of their supposed strategic value. Critics claim the list is too big, too inconsistent, and simply unrealistic.

Dr. Hylan B. Lyon, a CBEMA spokesman, formerly served as White House Science Adviser to four Presidents.

DR. HYLAN B. LYON: Anything can be used for military purposes. All technology in the U.S. is used by the military. What you have to do is decide which items make a significant contribution to the Soviet military. The weight of evidence is that a minicomputer or home computer won't make a significant contribution.

KROGH: Even some of the strongest supporters of tighter controls agree.

SENATOR NUNN: The government has to have credibility. And to have credibility, we have to have a list that's narrow enough that businesses believe that we really do know what we're doing. If the list is too long, if the list contains many items that can be purchased off the shelf, so to speak, in this country

or in other countries, then, to that extent, businesses get turned off.

KROGH: Moscow's access to advanced technology from other countries is a turn-off to American businessmen faced with stringent export controls. They point out that U.S. efforts to block construction of the Soviet gas pipeline failed precisely because France, Germany, and other members of the West's Coordinating Committee on Trade, called COCOM, refused to withhold their own technology from Moscow.

DR. LYON: You can make the assertion that almost any technology that the U.S. has also exists within COCOM. So if the Soviets want to acquire Western technology, they can acquire it from any one of those sources.

REP. BONKER: If we're going to say to a U.S. manufacturer, "You can't export because this is a dual-use item," or whatever; and France and Japan and England and West Germany and other countries don't comply with similar license requirements, then the only result of the program is to injure U.S. industry.

KROGH: U.S. industry is concerned that the Administration is trying to launch an all-out economic war against the Soviet Union. They don't think such a war can be won. They don't think they should be used to fight it. But they fear that high technology, the U.S. trump card in the highly competitive world of international trade, can be squandered by restricting instead of promoting exports.

But the final battlefield will be in Congress, as it moves toward renewal of the Export Administration Act, which expires in the fall, legislation which, unexpectedly, is becoming a focal point of U.S. policy toward the Soviet Union.

REP. BONKER: There are hawks in the Congress and hawks in the Administration who would like to see a cutoff of almost all our high technology, who have rather paranoid sentiments about the so-called hemorrhaging of our technology.

SENATOR NUNN: The whole thing is, you're not paranoid if they're really after it. And I think the Soviets really are after our technology.